



# **Security Certification Challenges in a Cloud Computing Delivery Model**

## **Systems and Software Technology Conference**

**April 27, 2010**

***Elizabeth Brown  
Chris Braganza  
Dr. Michael Martin  
Sri Vasireddy***

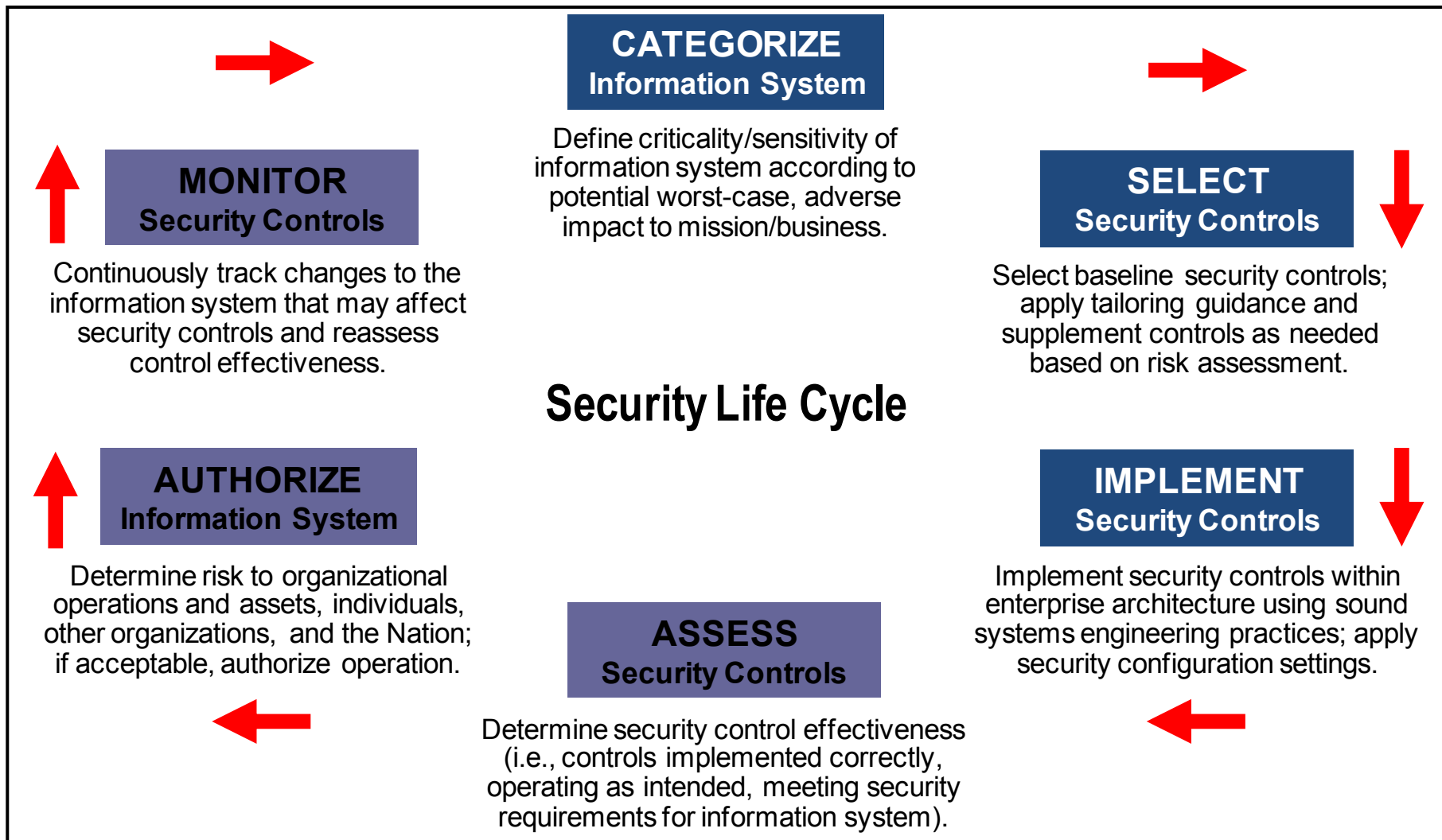
Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>27 APR 2010</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2010 to 00-00-2010</b>	
4. TITLE AND SUBTITLE <b>Security Certification Challenges in a Cloud Computing Delivery Model</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>MITRE,202 Burlington Road,Bedford,MA,01730-1420</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>19</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# Current Thinking...

---

- **“Cloud computing will be as influential as E-business.” - Gartner**
- **“It's the modern version of the timesharing model from the 1960s...” - Bruce Schneier**
- **“We can no more see the full impact of the cloud than Henry Ford foresaw the impact of his desire to produce more cars in less time.” - Russ Daniels**
- **“I think cloud computing has some security implications, but nobody really has a handle on what cloud computing even is.” - Marcus Ranum**

# NIST Risk Management Framework



# Impact Level Drives Control Selection

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<b><i>Confidentiality</i></b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Integrity</i></b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Availability</i></b> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

# 18 Security Control Families (NIST SP 800-53)

IDENTIFIER	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

## DOD IA Control Subject Areas (DODI 8500.2)

Abbreviation	Subject Area Name
DC	Security Design & Configuration
IA	Identification and Authentication
EC	Enclave and Computing Environment
EB	Enclave Boundary Defense
PE	Physical and Environmental
PR	Personnel
CO	Continuity
VI	Vulnerability and Incident Management

# Cloud Assurance—What will it take?

---

- **“...the certainty that a Service Provider can operate their cloud offering at a prescribed level.”**
- **Assurance is the grounds for confidence that the security controls implemented are effective in their application.**
- **For low-impact systems, the assurance requirement is that “the security control is in effect and it meets explicitly identified functional requirements in the control statement.”**
- **The controls are in place with the expectation that no obvious errors exist, and as flaws are discovered, they are discussed in a timely manner.**

# Issues and Assumptions

---

## ■ Issues

- Applicable cloud security standards
- Compensating security controls to mitigate
- Customers and service provider actions to achieve cloud assurance

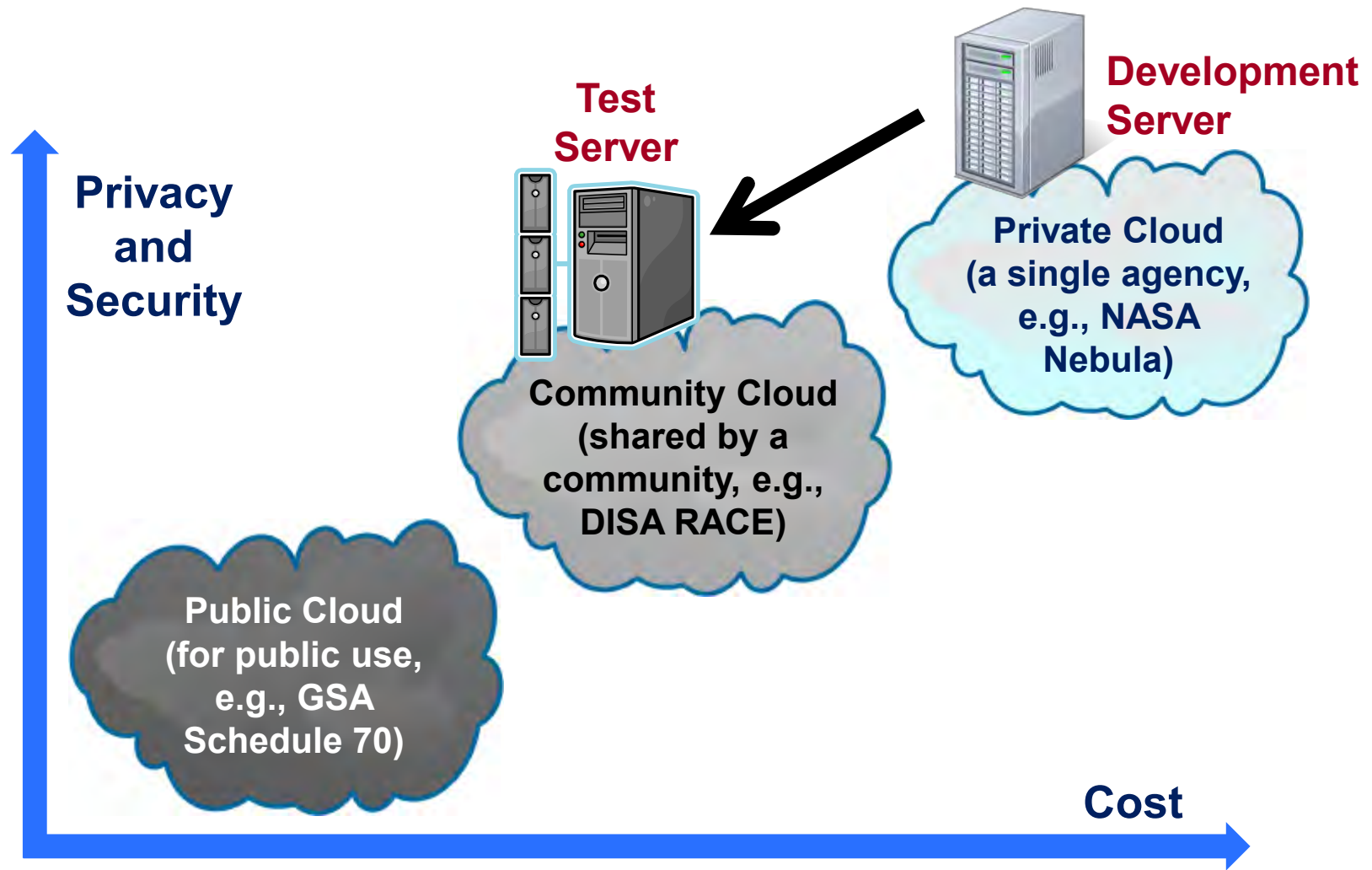
## ■ Assumptions

- NIST SP 800-53 security controls for a low-impact system





# Example of Low-Risk IaaS in Hybrid Cloud Deployment

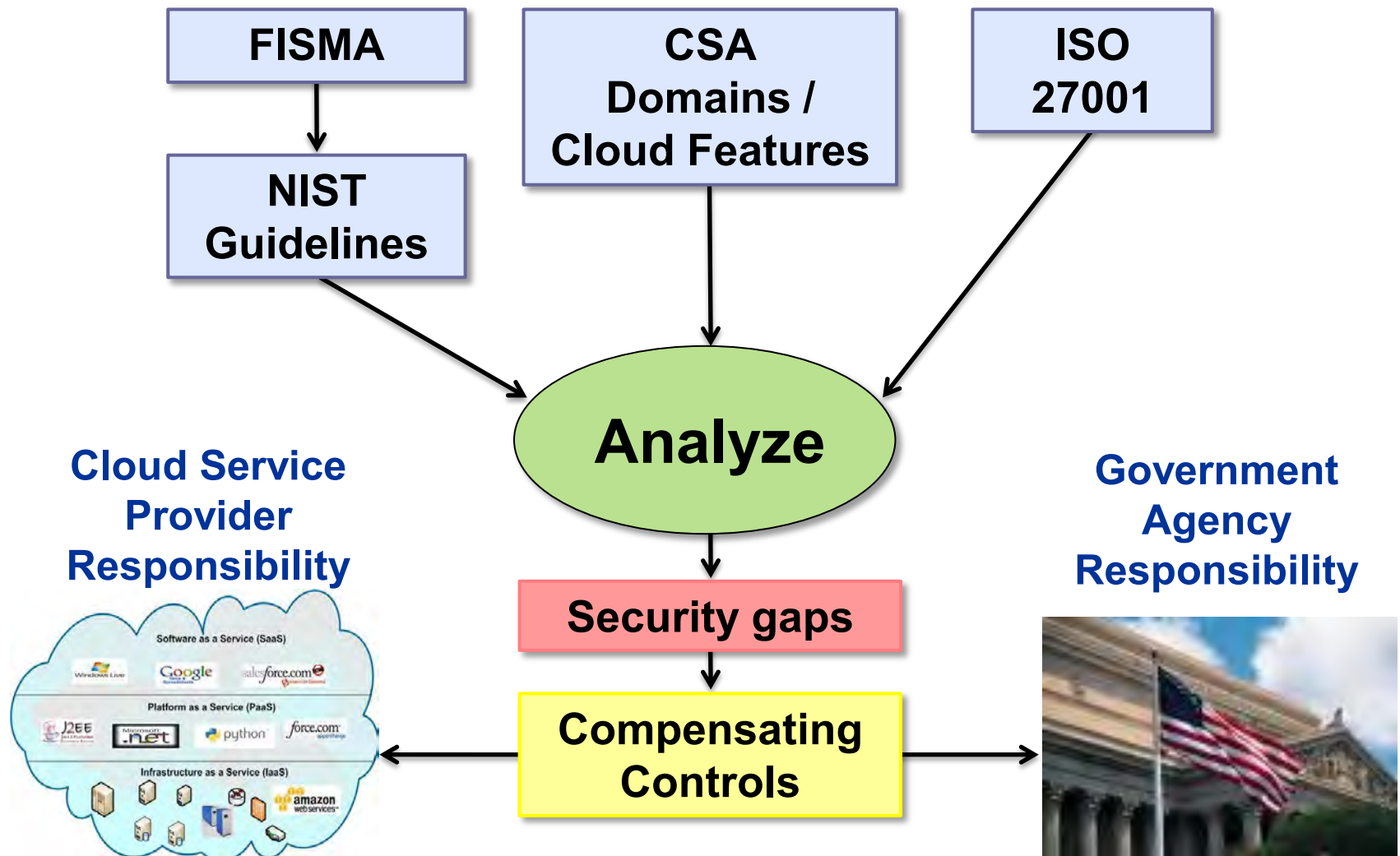


# Relevant Security Standards, Certifications, and Guidance

---

- **NIST SP 800 series**
- **ISO/IEC 27001 framework**
- **Cloud Security Alliance**
- **Statement of Accounting Standards, number 70 (SAS-70)**

# Cloud Security Certification Analysis



# Criteria for Difficulty of NIST 800-53 Control Family Certification Characteristics

---

Least Difficult	Most Difficult
<ul style="list-style-type: none"><li>• Mature practices exist</li><li>• No integration issues</li><li>• Technology is available if necessary</li><li>• Compensating controls are unnecessary</li></ul>	<ul style="list-style-type: none"><li>• Concepts and theory exist but with immature implementation methods</li><li>• Technology integration issues that impede implementation</li><li>• Compensating controls that are difficult to implement</li></ul>

# Results Categorization of NIST SP 800-53 Control Families

---

Least Difficult	Most Difficult
<ul style="list-style-type: none"><li>• Awareness and Training (AT)</li><li>• Audit and Accountability (AU)</li><li>• Physical and Environmental Protection (PE)</li><li>• Personnel Security (PS)</li><li>• Contingency Planning (CP)</li><li>• Incident Response (IR)</li><li>• Maintenance (MA)</li><li>• Planning (PL)</li><li>• Program Management (PM)</li><li>• System and Services Acquisition (SA)</li><li>• System and Information Integrity (SI)</li></ul>	<ul style="list-style-type: none"><li>• Security Assessment and Authorization (CA)</li><li>• System and Communications Protection (SC)</li><li>• Risk Assessment (RA)</li><li>• Media Protection (MP)</li><li>• Identification and Authentication (IA)</li><li>• Access Control (AC)</li><li>• Configuration Management (CM)</li></ul>

# Description of Most Difficult Results

---

Most Difficult
<ul style="list-style-type: none"><li>• <b>Security Assessment and Authorization (CA)</b><ul style="list-style-type: none"><li>– No mandate</li><li>– No metrics</li><li>– Integration issues unknown</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>System and Communications Protection (SC)</b><ul style="list-style-type: none"><li>– Boundary protection not enforced</li><li>– Lack of FIPS 140-2 support</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>Risk Assessment (RA)</b><ul style="list-style-type: none"><li>– No metrics</li><li>– Transparency required</li><li>– Unique for every instance</li></ul></li></ul>

# Description of Most Difficult Results

---

Most Difficult
<ul style="list-style-type: none"><li>• <b>Media Protection (MP)</b><ul style="list-style-type: none"><li>– Inconsistent protection methods</li><li>– Unverifiable data destruction and reuse methods</li><li>– Data aggregation vulnerabilities</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>Identification and Authentication (IA)</b><ul style="list-style-type: none"><li>– LDAP and Active directory integration issues</li><li>– Immature concepts</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>Access Control (AC)</b><ul style="list-style-type: none"><li>– Customer configuration challenges</li><li>– Transparency required</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>Configuration Management (CM)</b><ul style="list-style-type: none"><li>– Patch management not mandated</li><li>– No metrics</li></ul></li></ul>

# Compensating Controls

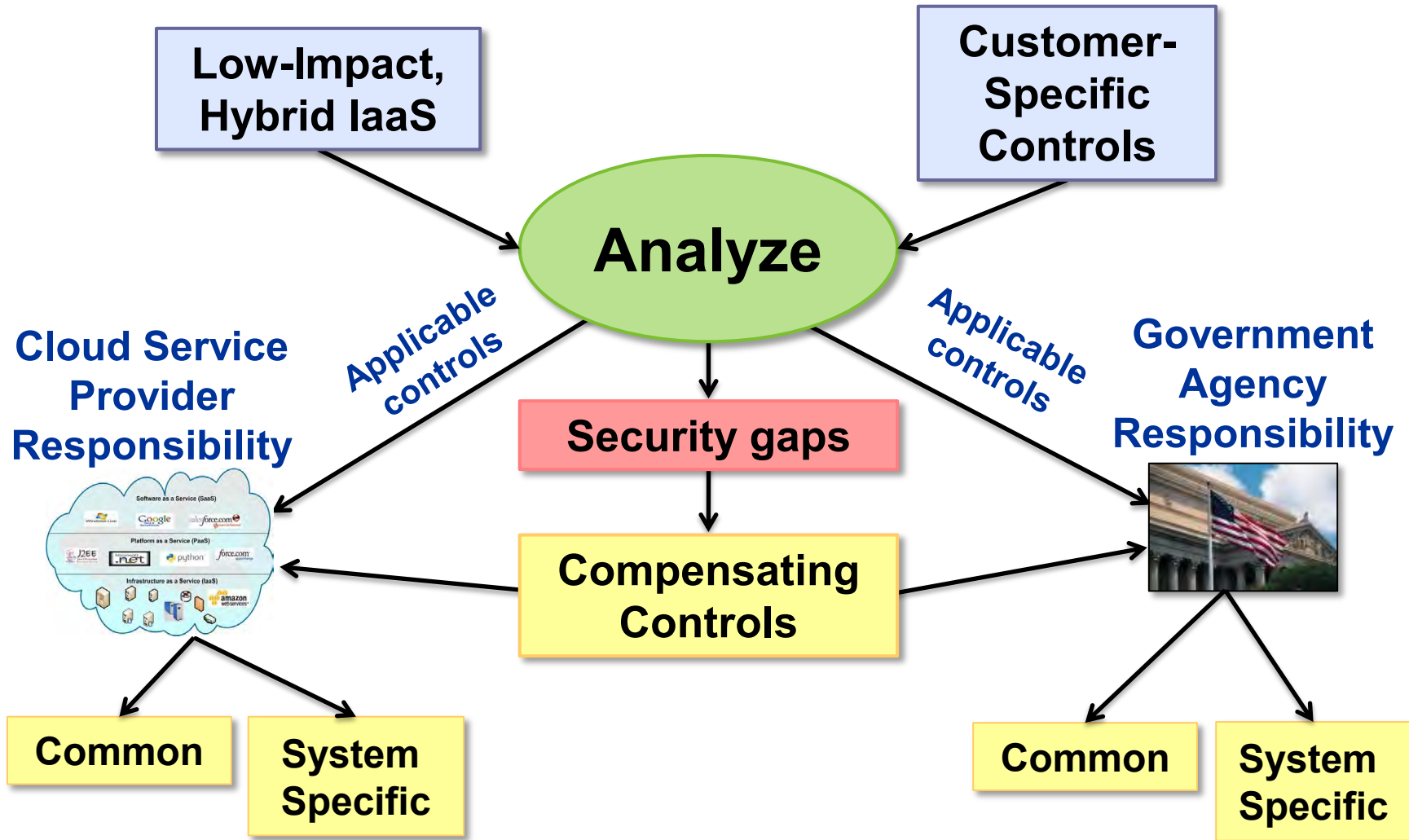
Unmet Control	Compensating Control	Customer Responsibility	Service Provider Responsibility
No certification mandate	Conduct a third-party assessment periodically	Require CA in SLA	Publish results. Provide Security Architecture.
Boundary protection not enforced	Enact strong Denial of Service (DoS) protection	Require DoS in SLA	Enable DoS to the edge
No RA mandates or metrics	Evaluate risk at a granular level	Ensure satisfactory risk mgmt methods	Be subject to an RA
Unverifiable protection and data destruction methods	Sanitize media before contract termination. Encrypt data to prevent disclosure.	Establish frameworks against attacks	Test for audit logging and reports



# Compensating Controls (concluded)

Unmet Control	Compensating Control	Customer Responsibility	Service Provider Responsibility
Access Control configuration is challenging	Define an access schema before deploying data to the cloud	Categorize. Define roles. Install IDS, Firewalls.	Deny all access default
Integration issues with LDAP and AD	Use identity management standards such as SAML and WS-Federation	Configure user and group policies on a AAA server	Support SAML and XACML
Patch management not mandated	Be proactive with vulnerability protection. Institute adequate patch management policies and procedures.	Conduct vulnerability assessments. Enforce NAC prerequisites.	Support dynamic analysis web application security tools

# Model - Allocate controls, identify gaps, assign responsibility for compensation




# Future Responsibilities Roadmap

---

Service Providers	Customers	Standards Bodies
<ul style="list-style-type: none"><li>• Service providers must build security into the service offering</li><li>• Service providers must provide transparent SLAs</li><li>• Service providers must allow for independent security assessments</li></ul>	<ul style="list-style-type: none"><li>• Customers eager to migrate must accept some risks</li><li>• Customers must be wary of SLAs</li></ul>	<ul style="list-style-type: none"><li>• NIST-leading Cloud Computing Security Working Group to establish baseline standards and authorization process for public clouds</li><li>• Cloud Security Alliance (industry group) seeking to establish security guidelines</li></ul>

# Contact Information

---



**Elizabeth Brown [ebrown@mitre.org](mailto:ebrown@mitre.org)**  
**Chris Braganza [braganza@mitre.org](mailto:braganza@mitre.org)**